ON SETS OF INTEGERS WHICH CONTAIN NO THREE TERMS IN ARITHMETICAL PROGRESSION

BY F. A. BEHREND

DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF MELBOURNE

Communicated October 18, 1946

Let S be a set of non-negative integers $\leq N$ no three of which form an arithmetical progression (i.e., $A + A' \neq 2A''$ for any three distinct terms of S). Let $\nu(N)$ denote the maximum number of terms of such a "progression-free" set. Salem and Spencer[1] proved that for $\epsilon > 0$ and sufficiently large N

$$\nu(N) > N^{1 - \frac{\log 2 + \epsilon}{\log \log N}}.$$

I will show in this note that, by a modification of their method, the better estimate

$$\nu(N) > N^{1 - \frac{2\sqrt{2 \log 2} + \epsilon}{\sqrt{\log N}}}$$

can be obtained.

For any integers $d \geqslant 2$, $n \geqslant 2$, $k \leq n(d - 1)^2$ consider the set $S_k(n, d)$ of all numbers of the form

$$A = a_1 + a_2(2d - 1) + \ldots + a_n(2d - 1)^{n-1}$$

where the "digits" a_i are integers subject to the conditions

$$0 \leq a_i < d \tag{i}$$

$$(\text{norm } A)^2 = k \tag{ii}$$

where

$$\text{norm } A = \sqrt{a_1^2 + a_2^2 + \ldots + a_n^2}.$$

This set is progression-free; for suppose $A + A' = 2A''$ for A, A', A'' in $S_k(n, d)$ then

$$\text{norm } (A + A') = \text{norm } (2A'') = 2\sqrt{k}$$

and

$$\text{norm } A + \text{norm } A' = 2\sqrt{k}.$$

Thus, in the triangular inequality

$$\text{norm } (A + A') \leq \text{norm } A + \text{norm } A'$$

equality holds which is only possible if $(a_1, a_2, \ldots, a_n)$ and $(a_1', a_2', \ldots, a_n')$ are proportional and, as their norms are equal, identical, i.e., if $A = A' = A''$.

There are d^n different systems $(a_1, a_2, \ldots, a_n)$ satisfying (i) and $n(d-1)^2 + 1$ possible values of k; hence for some $k = K$, $S_k(n, d)$ must contain at least

$$\frac{d^n}{n(d-1)^2+1} > \frac{d^{n-2}}{n}$$

terms; as all these terms are $< (2d-1)^n$ we have

$$\nu((2d-1)^n) > \frac{d^{n-2}}{n}.$$

Let N be given; choose $n = \left[\sqrt{\frac{2 \log N}{\log 2}}\right]$, and d such that

$$(2d-1)^n \leq N < (2d+1)^n.$$

Then,

$$\nu(N) \geqslant \nu((2d-1)^n) > \frac{d^{n-2}}{n} > \frac{(N^{1/n}-1)^{n-2}}{n2^{n-2}} = \frac{N^{1-(2/n)}}{n2^{n-2}}(1 - N^{-1/n})^{n-2},$$

and, for sufficiently large N,

$$\nu(N) > \frac{N^{1-(2/n)}}{n2^{n-1}} = N^{1 - \frac{2}{n} - \frac{\log n}{\log N} - \frac{(n-1)\log 2}{\log N}} > N^{1 - \frac{2\sqrt{2 \log 2} + \epsilon}{\sqrt{\log N}}}$$

for any $\epsilon > 0$.

[1] Salem, R., and Spencer, D. C., "On Sets of Integers Which Contain No Three Terms in Arithmetical Progression," these PROCEEDINGS, 28, 561–563 (1942).